R. Alexander Saveri (SBN 173102)
Geoffrey C. Rushing (SBN 126910)
Cadio Zirpoli (SBN 179108)
Sarah Van Culin (SBN 293181)
SAVERI & SAVERI, INC.
706 Sansome Street
San Francisco, CA 94111
Telephone: (415) 217-6810
Facsimile: (415) 217-6813
Email: rick@saveri.com; geoff@saveri.com;
cadio@saveri.com; sarah@saveri.com

Randall Robinson Renick (SBN 179652)
HADSELL STORMER RICHARDSON & RENICK, LLP
128 N. Fair Oaks Ave.
Pasadena, CA 91103
Telephone: (626) 585-9600
Facsimile: (626) 577-7079
Email: rrr@hadsellstormer.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

MICHAEL BRANCH, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, vs. EQUIFAX, INC. Defendant.	CASE NO.: 3:17-cv-05429 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, Michael Branch, individually and on behalf of all those similarly situated, brings this action for damages and equitable relief against Equifax, Inc. and alleges, based upon the investigation of counsel and on information and belief, as follows:

I. OVERVIEW

1. On September 7, 2017, Equifax, Inc. ("Equifax" or "Defendant") announced the largest data breach in history. Hackers used a known vulnerability in an Equifax website application to gain access to confidential personal information including names, Social Security numbers, addresses, birth dates, and, in some instances, driver's license numbers of some 143 million Americans.

2. After discovering the hack on July 29, 2017, Equifax waited 40 days to make news of the data breach public, leaving consumers at heightened risk of identity theft for over a month.

3. The hackers were able to gain access to this confidential personal information by exploiting a known Apache Struts vulnerability that had been publicized—and a patch issued—two months before the hack occurred.

4. Equifax's negligence in failing to repair this known vulnerability and its failure to take reasonable security measures to protect consumer data means millions of Americans are now at risk of identity theft and have incurred expenses and inconvenience in addressing the consequences of this data breach.

5. Plaintiff and members of the proposed Classes have suffered harm and face the imminent risk of future harm, including:

a. Costs associated with the detection and prevention of identity theft and unauthorized use of their confidential personal information;

b. Costs incurred in and the loss of productivity from taking time to address, mitigate, and deal with the actual and future consequences of this data breach, including finding and challenging fraudulent changes to debit and credit accounts, cancelling credit cards,

imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all of the issues resulting from this data breach;

c. Theft of their personal information;

d. Imminent, impending threat of fraud and identity theft as a result of their personal information being in the hands of hackers and already misused and sold on the Internet and/or black market;

e. Loss of use of and access to their account funds and costs associated with their inability to obtain money from their accounts or being limited in the amount of money they could obtain from their accounts, including missing payments on bills and loans, late charges and fees, and adverse effects on credit including decreased credit scores and adverse credit notations;

f. Damage to and the diminution in value of confidential personal information entrusted to Equifax for the sole purpose of reporting and/or monitoring their credit profile with the mutual understanding that Equifax would safeguard Plaintiff and the Class members' data against theft and not allow access and misuse of their data by others;

g. Any money paid for products purchased from Equifax (such as credit monitoring or credit score inquiries) at any time after July 29, 2017 when the data breach was discovered by Equifax because they would not have engaged Equifax for those services if Equifax had disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' confidential personal information; and

h. Continued risk to their confidential personal information that is still in Equifax's possession and which is at risk of further breaches so long as Equifax fails to undertake adequate measures to protect the data.

6. Plaintiff brings this action on behalf of himself individually and all those similarly situated in order to redress the harm already suffered by the class and to prevent future failures by Equifax to protect consumer data. Plaintiff seeks damages and equitable relief.

II. PARTIES

7. Plaintiff, Michael Branch, is a resident of Los Angeles County, California, whose

confidential personal information was included in the data breach of Equifax's systems and disclosed to unauthorized third parties and Mr. Branch was harmed as a direct and proximate result of the conduct alleged herein. Mr. Branch entered his last name and the last six digits of his social security number into the Equifaxsecurity2017.com "Check Potential Impact" webpage and was informed that his confidential personal information may have been impacted by the data breach.

8. Defendant, Equifax, Inc., is a Georgia corporation with its headquarters in Atlanta, Georgia. Equifax, Inc. is registered with the California Secretary of State's office as an Active Foreign Stock Corporation. Equifax conducts business throughout the United States, including in the Northern District of California, and did so during the Class Period.

9. Equifax has offices in California including in Moorpark, near Los Angeles. TrustedID, Inc., is owned by Equifax and is a Delaware Corporation with its principal office in Palo Alto, California.

III. JURISDICTION AND VENUE

10. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because the matter in controversy exceeds $5 million, exclusive of interest and costs, and at least one plaintiff and the defendant are citizens of different states. There are more than 100 putative class members.

11. This Court has jurisdiction over Equifax because Equifax is authorized to and regularly does conduct business in California and has sufficient minimum contacts with California. Equifax transacted business throughout the United States, including in this District; sold or marketed its products throughout the United States, including in this District; and purposefully availed itself of the laws of the United States and the State of California. Equifax reported to the Office of the Attorney General for the State of California that approximately 15,178,887 California residents were potentially impacted by the data breach.

12. Venue is proper in this District because Equifax is licensed to do business in and is doing business in this District, the Court has personal jurisdiction over Equifax, and because a

substantial part of the events giving rise to the claim occurred in this District.

13. This action is not subject to arbitration. Equifax's website states:

> [E]nrolling in the free credit file monitoring and identity theft protection that we are offering as part of this cybersecurity incident does not waive any rights to take legal action. We removed that language from the Terms of Use on the website, www.equifaxsecurity2017.com. The Terms of Use on www.equifax.com do not apply to the TrustedID Premier product being offered to consumers as a result of the cybersecurity incident.[1]

IV. FACTUAL ALLEGATIONS

14. There are three major credit reporting agencies in the United States—Equifax, Experian, and TransUnion.[2] These agencies are responsible for running the reports that are used to calculate consumers' credit scores; impacting their ability to get a mortgage, buy a car, or engage in any number of other financial transactions.[3]

15. Private information is Equifax's lifeblood. Equifax organizes and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide. Its database includes employee data contributed from more than 7,100 employers.[4] Equifax operates or has investments in 24 countries spanning North America, Central and South America, Europe and the Asia Pacific region.[5] Last year, Equifax made $3.1 billion in revenue.[6]

16. Equifax is well aware of the private, sensitive nature of the information it stores. The Equifax website describes identity theft as "when someone steals your personal information – such as your name, Social Security number, and date of birth – typically to hijack your credit and use it to open up new credit accounts, take out loans in your name, or access your bank or retirement accounts."[7] The Equifax website also describes how this stolen information is used:

---

[1] https://www.equifaxsecurity2017.com/2017/09/11/progress-update-consumers-2/ [A Progress Update for Consumers, September 11, 2017]
[2] https://www.nytimes.com/2017/09/08/business/equifax.html
[3] https://www.nytimes.com/2017/09/08/business/equifax.html
[4] http://www.equifax.com/about-equifax
[5] http://www.equifax.com/about-equifax
[6] https://www.nytimes.com/2017/09/08/business/equifax.html
[7] https://www.equifax.com/personal/education/identity-theft/what-is-identity-theft

> An identity thief can even use your personal information to steal your tax refunds, seek medical services, or commit crimes in your name. Once an identity thief has access to your personal information, he or she can also:
>
> Open new credit card accounts with your name, Social Security number and date of birth. When the thief charges to the credit cards and leaves the bills unpaid, the delinquency will be reported to your credit report and could impact your credit score;
>
> Open a bank account in your name and write bad checks on the account;
>
> Create counterfeit checks or debit cards and use them to drain your existing bank accounts;
>
> File for bankruptcy under your name to avoid paying debts;
>
> Set up a phone, wireless, or other utility service in your name.[8]

17. After outlining this parade of horribles for consumers, Equifax suggests consumers "Consider these Products" including "Equifax ID Patrol™," "Equifax ID Patrol™ Premier" and "Equifax Complete™ Advantage Plan" that claim to help consumers monitor their credit and protect their identity.

18. The Equifax data breach is one of the largest breaches ever.[9] From mid-May through July 2017, "Criminals exploited a U.S. website application vulnerability to gain access to certain files" held by Equifax.[10] These files contained the names, Social Security numbers, birth dates, and addresses and, in some instances, driver's license numbers of some 143 million U.S. consumers.[11] In addition, the credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with the personal identifying information for approximately 182,000 U.S. consumers were accessed.[12] Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents.[13]

---

[8] https://www.equifax.com/personal/education/identity-theft/what-is-identity-theft
[9] http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX
[10] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628
[11] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628
[12] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628
[13] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628

19. Approximately 15,178,887 California residents were potentially affected by this data breach.[14]

20. Equifax has stated that this breach was due to an Apache Struts vulnerability: "The vulnerability was Apache Struts CVE-2017-5638."[15]

21. The vulnerability identified by Equifax as the cause of this data breach had been discovered and patched some two months before the data breach.[16] Equifax did not update its website applications to fix this issue, despite reports back in March that hackers were actively targeting this vulnerability.[17] Instead Equifax's website indicates that patching of this vulnerability did not occur until late July, after the breach had occurred:

> On July 29, 2017, Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application. In response, the Security team investigated and blocked the suspicious traffic that was identified.
>
> The Security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, the company took offline the affected web application that day.
>
> The company's internal review of the incident continued. Upon discovering a vulnerability in the Apache Struts web application framework as the initial attack vector, Equifax patched the affected web application before bringing it back online.[18]

22. "Apache Structs is free, open-source software used to create Java web applications."[19] However, as noted by Boris Chen, vice president of engineering at tCell in an interview with USA Today: "A single vulnerability in a web component should not result in millions of highly sensitive records being exfiltrated. Security controls should have existed at

[14] https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax-data-breach; https://oag.ca.gov/system/files/Equifax%20-%20CA%20Letter_0.pdf
[15] https://www.equifaxsecurity2017.com/2017/09/13/progress-update-consumers-4/
[16] https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/
[17] https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/
[18] https://www.equifaxsecurity2017.com/ [Consumer Update, September 15, 2017]
[19] https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-answers-and-some-questions/658343001/

many points along the way to stop such a catastrophic outcome."[20]

23. Equifax discovered the data breach on July 29, 2017 but did not make this information public until September 7, 2017, some 40 days later, when Equifax issued a press release.[21]

24. While the public was kept in the dark about this massive breach, Equifax executives apparently were not. Three senior executives "sold $1.8 million worth of shares in the days after Equifax discovered the breach."[22] Equifax shares have dropped 32 percent since the company disclosed the breach.[23]

25. Equifax knew or should have known that its systems were at-risk of hacking attacks based on previous attacks and reports that its internal system had weaknesses. Equifax failed to improve its data security after two data breaches that occurred in the last year: one in which hackers took valuable W-2 tax and salary data from the Equifax website and, in another, hackers took W-2 tax data from an Equifax subsidiary called TALX. Cybersecurity professionals interviewed by the New York Times concluded that there should have been more controls in place to prevent the most recent data breach, especially in light of these prior incidents.

26. The first Equifax security breach, which led to a class action lawsuit, stemmed from a May 2016 incident in which Equifax's W-2 Express website was breached, leading to the leak of 430,000 names, addresses, social security numbers, and other information. Equifax had clients' employees access their data with default PIN numbers made up of the last four digits of their social security number and four digit year of birth; assigned PIN numbers that were exceedingly easy for criminals to find on the internet. Equifax agreed to fix the underlying issue that led to this data breach, although it is unclear if the vulnerability has yet to be adequately addressed.

[20] https://www.usatoday.com/story/tech/2017/09/12/how-did-equifax-breach-happen-here-some-answers-and-some-questions/658343001/
[21] https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628
[22] https://www.nytimes.com/2017/09/08/business/equifax.html
[23] http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX

27. The second prior Equifax data breach involving TALX was especially alarming because Equifax failed to discover that breach for almost a year—from April 17, 2016 through March 29, 2017. This breach was not publicly disclosed until May 2017. That security breach related to hackers using personal information to guess client customer questions and ultimately reset their 4-digit PIN to gain access to customers' tax data.

28. Equifax also suffered smaller data breaches in January 2017 concerning LifeLock customer credit information, and a 2013-2014 breach of credit reports using personal information. In 2016, a vulnerability to cross-site scripting was discovered. Cross-site scripting, also known as XSS, is a process by which an attacker could send a link they create to users who would click on the link and long on to the website, revealing their user names and passwords and jeopardizing their personal information.

29. Security experts Kenneth White and Kevin Beaumont found that Equifax may have been susceptible to attacks because it uses old and discontinued technologies, like Netscape, IBM Websphere, Apache Struts, and Java. The vulnerabilities of those programs should have been addressed sooner given the sensitivity of information and the risk. AlienVault security advocate, Javvad Malik notes that "[c]ompanies like Equifax should know very well that data is the lifeblood of the organization and its crown jewels."

30. There are several governmental investigations already underway. The FTC has confirmed that they are investigating the Equifax data breach.[24] The Consumer Financial Protection Bureau is also investigating Equifax. The chairmen of the House Committee on Science, Space, and Technology and the House Committee on Oversight and Government Reform have said that their respective committees will investigate the Equifax data breach and have requested that Equifax produce documents by September 28.[25] Equifax CEO Richard Smith is scheduled to appear at a hearing on the House Subcommittee on Digital Commerce and

[24] http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX; https://www.usatoday.com/story/money/2017/09/14/ftc-investigating-equifax-over-data-breach/665550001/

[25] http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX

Consumer Protection on October 3.[26] The Federal Bureau of Investigation has opened an investigation into the breach, along with nearly 40 states.[27]

31. The FTC website suggests that people consider freezing their credit reports in light of this data breach, but this can be inconvenient in that it keeps consumers from opening new accounts unless they unfreeze them days in advance.

32. Further, even if consumers freeze their credit reports with Equifax, they must also freeze them for Experian and TransUnion as well to give them the best protection.

33. To add cost to this inconvenience of freezing credit reports, in some states these companies require consumers to pay a fee to freeze and unfreeze their credit reports.

34. Unfortunately, even if consumers freeze their credit reports, they are not protected from fraudulent tax returns being filed with their information or people using their credit cards.

35. Security analyst at Gartner, Avivah Litan is quoted in a USA Today article as saying that instead of checking credit card statements monthly, people need to now check them weekly and be hyper-vigilant if their information has been jeopardized. This is a further inconvenience that those attached by this data breach must endure.

36. In addition to common fears relating to identity theft like credit card use, people opening accounts in another person's name, and harm to a credit score, consequences like medical identity theft (fake IDs used to pay for procedures and surgeries), tax fraud (filing false tax returns to profit from refunds), and synthetic identity theft (combining information from multiple victims to create a new identity) are also possible because of the depth of information stolen.

V. CLASS ALLEGATIONS

37. Plaintiff brings this class action pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(2) and (b)(3) on his own behalf and as representative of the following classes of

[26] http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX; https://www.usatoday.com/story/money/2017/09/14/ftc-investigating-equifax-over-data-breach/665550001/

[27] http://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX

persons and entities (the "Classes").

38. A nationwide "Negligence Class" seeking damages, equitable and injunctive relief:

> All persons and entities in the United States whose confidential personal information was compromised as a result of the data breach publically announced by Equifax on September 7, 2017. Excluded from the Class is Defendant, its parent companies, subsidiaries and affiliates, employees of Defendant, including its officers and directors; and any judge or jurors assigned to this case.

And a "California Class" seeking damages, equitable and injunctive relief:

> All residents of the State of California whose confidential personal information was compromised as a result of the data breach publically announced by Equifax on September 7, 2017. Excluded from the Class is Defendant, its parent companies, subsidiaries and affiliates, employees of Defendant, including its officers and directors; and any judge or jurors assigned to this case.

39. The proposed classes are each so large that joinder of all members is impracticable. Class members are also dispersed geographically, both throughout California and the U.S. While Plaintiff does not know the exact number of members of the Class, Plaintiff understands that some 143 million U.S. consumers were affected by the breach, with over 15 million of those consumers being California residents. The number of affected consumers was reported to the California Department of Justice, Office of the Attorney General by Equifax. The class members thus appear readily ascertainable from records in Equifax's possession, custody and control. Indeed, Equifax has established a website specifically designed to allow consumers to check if their data was compromised in the data breach.[28]

40. Common questions of law and fact exist as to all members of each Class. This is particularly true given the nature of the data breach, which affected all members of each Class, thereby making appropriate relief with respect to each Class as a whole. Such common questions of law and fact include but are not limited to:

a. Whether Equifax engaged in the unlawful conduct as herein alleged;

[28] https://www.equifaxsecurity2017.com/

b. Whether Equifax owed a duty to the class members to protect their confidential personal information;

c. Whether Equifax breached their duty to protect the confidential personal information;

d. Whether Equifax knew or should have known of the vulnerabilities in its systems;

e. Whether Equifax was negligent in failing to address those vulnerabilities;

f. Whether Equifax knew or should have known about the vulnerabilities in its systems before the data breach occurred;

g. Whether Equifax had a duty to notify class members of the data breach in a timely manner;

h. Whether Equifax notified class members of the data breach in a timely manner;

i. The appropriate injunctive and related equitable relief for the Class; and

j. The appropriate class-wide measure of damages.

41. Plaintiff's claims are typical of the claims of the members of the Class, and Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff and all members of the Class are similarly affected by Equifax's conduct as their personal identifying information was breached as a result of Equifax's conduct and they were harmed as a result of that conduct.

42. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class. Plaintiff's interests are coincident with, and not antagonistic to, those of the other Class members. Plaintiff is represented by counsel, who are competent and experienced in the prosecution of large-scale class action litigation.

43. The questions of law and fact common to the members of the Class are predominant and outweigh those questions affecting only individual members, including legal and factual issues relating to liability and damages.

44. Class action treatment is a superior method for the fair and efficient adjudication of this litigation. With 143 million putative class members, class treatment will allow this enormous number of similarly situated potential plaintiffs to prosecute their common claims in a

single forum in the most efficient manner. This will avoid the inevitable duplication of evidence, effort, and expense that numerous individual actions would involve. The benefits of proceeding through the class action mechanism, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually and significantly reducing the burden on the court system of trying these cases individually, far outweigh any difficulties that may arise in the management of this class action.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION: NEGLIGENCE

(Nationwide Negligence Class)

45. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

46. Equifax owed a duty to Plaintiff and the Class to protect the confidential personal information stored on Equifax's systems. Equifax was well aware of the value of this information and owed a duty to consumers to take all reasonable steps to ensure that the information was protected and safeguarded from hacking attacks. Indeed, Equifax created the risk of hacking: its business is dedicated to collecting and analyzing sensitive information about consumers.

47. This duty to protect consumers' data is reflected in the law. California Civil Code, Section 1798.81.5(b) requires that "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

48. The risk of hacking was reasonably foreseeable. Equifax's own website warns of the "sophisticated tactics" used by identity thieves to access personal information of the kind accessed in this data breach.[29] Equifax had previous warning that hackers were targeting the information in their possession and knew or should have known that they needed to take all

[29] https://www.equifax.com/personal/education/identity-theft/how-to-protect-against-identity-theft

reasonable steps to protect this information. The *New York Times* reported that last year, W-2 tax and salary data was hacked from an Equifax website, while earlier this year, W-2 tax data was hacked from TALX, an Equifax subsidiary.[30]

49. Equifax knew or should have known that the vulnerability used by the hackers in the data breach existed in their website applications. The information concerning the particular website application vulnerability exploited in this data breach was freely available online as soon as the vulnerability was discovered, along with reports that hackers were targeting this vulnerability to access sensitive information. Equifax failed to secure its website applications against these attacks, even though information concerning the vulnerability and how to patch it was available two months before the data breach happened. As stated on Equifax's website, this patch was not done until the days following Equifax's discovery of the data breach in late July. Equifax failed to take the necessary steps to protect consumer data.

50. Plaintiff and the Class members' confidential personal information would not have been compromised in this way if not for Equifax's failure to fulfill the duty it owed to consumers to take reasonable steps to protect their data from hacking.

51. Neither Plaintiff nor the other Class Members contributed to the data breach or Equifax's use of insufficient and below-industry standard security measures to safeguard confidential personal information.

52. It was foreseeable that Equifax's failure to exercise reasonable care in protecting the confidential personal information of consumers would result in Plaintiff and the other Class Members suffering harm related to the loss of their personal information.

53. In advertising their products to consumers, Equifax states unequivocally on their website: "being a victim of identity theft can be financially and emotionally devastating."[31] Plaintiff and members of the Class have been harmed by having their personal information accessed by unauthorized third parties. The full extent of the harm is unknown at this time but, at

[30] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html
[31] https://www.equifax.com/personal/education/identity-theft/how-to-protect-against-identity-theft

the very least, Plaintiff and members of the Class have been forced to incur expenses to protect themselves from identity theft, for example signing up for credit monitoring or fraud prevention services, and will face further expenses to address any identity theft that occurs as a result of Equifax's failure to keep consumer's personal information secure. As noted by Adam Levin, chairman of CyberScout, in a quote to the New York Times: "The collateral damage can be devastating, and when you are talking about Social Security numbers the only expiration date a Social Security number has is yours."[32]

54. Furthermore, Plaintiff and members of the Class face the ongoing risk of identity theft as a result of this data breach. In addition to the expenses incurred to protect themselves, as far as possible, from the use of their compromised data, Plaintiff and members of the Class now face the inconvenience of stepping up their own monitoring of their credit report and related activity to guard against signs of identity theft and the ongoing heightened risk of identity theft.

55. As a direct and proximate result of Equifax's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial. Plaintiff and the Class pray for relief as set forth below.

SECOND CAUSE OF ACTION: Violation of California Customer Records Act

(Cal. Civil Code §§ 1798.80, et. seq.)

(California Class)

56. Plaintiff incorporates and realleges, as through fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

57. Pursuant to California Civil Code, Section 1798.81.5(b), "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the information from unauthorized access, destruction, use, modification, or disclosure."

58. As described in detail above, Equifax failed to implement and maintain

[32] https://www.nytimes.com/2017/09/08/business/equifax.html

reasonable security procedures and practices to protect the confidential personal information it maintained. Equifax's failure to fix a vulnerability that it knew or should have known existed in its website applications meant that unauthorized third parties were able to access, use, and/or disclose consumers' data.

59. Furthermore, pursuant to California Civil Code, Section 1798.82(a), any agency that owns or licenses "computerized data that includes personal information" is required to disclose any breach of the security of their systems to any California resident (1) whose unencrypted personal information was acquired by an unauthorized person or (2) where both encrypted personal information and the encryption key or security credential were both acquired. This disclosure must be made "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

60. California Civil Code, Section 1798.82 (b) requires similar disclosures to the owner or licensee of the information where an agency maintains but does not own the personal information "immediately following discovery."

61. Equifax knew of the breach for approximately 40 days before it notified California consumers.

62. Plaintiff and the California Class were injured by these actions in that their personal information was accessed, used, and/or disclosed by unauthorized third parties. Plaintiff and the California Class have and will incur expenses to secure their private information and address any identity theft that occurs as a result of Equifax's failure to keep the personal information of California residents secure. In addition to the expenses incurred to protect themselves, as far as possible, from the use of their compromised data, Plaintiff and members of the Class now face the inconvenience of stepping up their own monitoring of their credit report and related activity to guard against signs of identity theft and the ongoing heightened risk of identity theft.

63. Plaintiff and the California Class seek monetary damages pursuant to California

Civil Code, Section 1798.84(b). Plaintiff and the California Class also seek injunctive relief pursuant to California Civil Code, Section 1798.84(e) to prevent any further violation of the California Customer Records Act as a result of Equifax's lax security. Plaintiff and the Class pray for relief as set forth below.

THIRD CAUSE OF ACTION: Violation of Unfair Competition Law

(Cal. Bus. & Prof. Code §§ 17200 et seq.)

(California Class)

64. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

65. Equifax's unlawful, unfair and/or fraudulent business acts and practices – particularly, their lax security in violation of the California Customer Records Act and negligence in safeguarding the private personal information of some 15 million California residents - harmed California consumers

66. Equifax's lax security measures are an unlawful violation of the California Customer Records Act and directly resulted in the harm suffered by Plaintiff and the California Class.

67. Equifax's delay in announcing the data breach is an unfair business practice that left California consumers at heightened risk of identity theft for over a month. While Equifax knew from July 29, 2017 that confidential personal information was accessed in the data breach, this information was not disclosed to California consumers until September 7, 2017. This unfair and improper delay in notifying California consumers of the breach left California consumers at risk of identity theft. The inexcusable nature of this delay is compounded by reports that senior Equifax executives sold off $1.8 million of stock after the breach happened but before news of the breach was made public.

68. Plaintiff and the California Class have and will suffer economic injury as a result of Equifax's unlawful, unfair and/or fraudulent business practices. Plaintiff and the California Class have and will incur expenses to secure their private information and address any identity

theft that occurs as a result of Equifax's failure to keep the confidential personal information of California residents secure. Plaintiff and the California Class now also face the inconvenience of vigilantly monitoring their credit report and use of their personal information for signs of identity theft and the ongoing heightened risk of identity theft.

69. The harm suffered by Plaintiff and the California Class is directly linked to Equifax's business acts and practices. Plaintiff and the California Class members' information would not have been compromised in this way if not for Equifax's failure to fulfill the duty it owed to consumers to take reasonable steps to protect their data from hacking.

70. Plaintiff and the California Class seek equitable relief directing full restitution of all revenues, earnings, profits, compensation and benefits which may have been obtained by Equifax as a result of its unlawful and unfair business acts and practices. Plaintiffs also seek injunctive relief enjoining Equifax from engaging in the unlawful and unfair business practices described herein in the future to ensure that Equifax takes all reasonable and necessary steps to protect the confidential personal information it gathers from future hacking attempts.

FOURTH CAUSE OF ACTION: Unjust Enrichment

(Nationwide Class)

71. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

72. Equifax knowingly received and retained benefits and funds from Plaintiff and class members by compiling and using their confidential personal information and from the amounts paid by any class members who purchased services from Equifax.

73. In addition, Equifax saved on the cost of providing adequate data security to Plaintiff and the Class members. Equifax's cost savings came at the direct expense of the security of Plaintiff and the Class members' confidential personal information.

74. Equifax appreciates and/or has knowledge of the benefits conferred upon it by Plaintiff and the other class members.

75. As a result of Equifax's wrongful conduct, as described in detail herein, Equifax has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the other Class members.

76. Equifax's unjust enrichment is traceable to and directly and proximately results from the wrongful conduct, as described in detail herein, including compiling and using Plaintiff and the other Class members' confidential personal information without employing reasonable security measures to keep that information safe from hackers.

77. It is inequitable to allow Equifax to retain the benefits they have received, and continue to receive from Plaintiff and the other Class members. Plaintiff and the Class members did not confer these benefits officiously or gratuitously and it would be inequitable and unjust for Equifax to retain these profits.

78. Plaintiff and the Class members seek restitution in the amount of Equifax's wrongfully obtained profits.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court:

A. Determine that this action may be maintained as a class action under Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure;

B. Direct that notice of this action, as provided by Rule 23(c)(2) of the Federal Rules of Civil Procedure, be given to the Class;

C. Appoint Plaintiff as Class Representative and his counsel of record as Class Counsel;

D. Enter judgment against Equifax and in favor of Plaintiff and the Class;

E. Adjudge and decree that the acts alleged herein by Plaintiff and the Class against Equifax constitute negligence, violation of the California Customer Records Act, violation of California's Unfair Competition Law, and unjust enrichment;

F. Award Plaintiff and the Class damages to the maximum extent allowed, including actual and statutory damages;

G. Award restitution, including Equifax's wrongfully obtained profits, payable to Plaintiff and the Class;

H. Award punitive damages, including treble and/or exemplary damages, to the maximum extent allowed;

I. Award Plaintiff and the Class equitable, injunctive and declaratory relief as appropriate under applicable laws, including an injunction permanently barring continuation of the conduct complained of herein, and mandating that Defendant and any successors in interest be required to adopt and implement appropriate systems, controls, policies and procedures to protect the confidential personal information of Plaintiff and the Class;

J. Award pre- and post-judgment interest at the highest legal rate;

K. Award Plaintiff and the Class members' reasonable attorneys' fees and costs of suit; and

L. Award such other and further relief as the Court may deem just and proper.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

VI. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: September 19, 2017

/s/ R. Alexander Saveri

R. Alexander Saveri (173102)
Geoffrey C. Rushing (126910)
Cadio Zirpoli (179108)
Sarah Van Culin (293181)
SAVERI & SAVERI, INC.
706 Sansome Street
San Francisco, CA 94111
Telephone: (415) 217-6810
Facsimile: (415) 217-6813
Email: rick@saveri.com;
geoff@saveri.com;
cadio@saveri.com; sarah@saveri.com

Randall Robinson Renick
HADSELL STORMER
RICHARDSON & RENICK, LLP
128 N. Fair Oaks Ave.
Pasadena, CA 91103
Telephone: (626) 585-9600
Facsimile: (626) 577-7079
Email: rrr@hadsellstormer.com